DEPARTMENT OF THE NAVY
NAVY PERSONNEL COMMAND
5720 INTEGRITY DRIVE
MILLINGTON TN 38055-0000

NAVPERSCOMINST 5510.1B
PERS-534
11 AUG 2009

NAVPERSCOM INSTRUCTION 5510.1B

From: Commander, Navy Personnel Command

Subj: NAVY PERSONNEL COMMAND (NAVPERSCOM) SECURITY PROGRAM

Ref: (a) SECNAV M-5510.36 of Jun 06
(b) SECNAV M-5510.30 of Jun 06
(c) OPNAVINST 5239.1B
(d) OPNAVINST 5530.14D
(e) BUPERSINST 5510.61B

Encl: (1) NAVPERSCOM Security Program

1. Purpose. To implement Navy Personnel Command (NAVPERSCOM) security policy and procedural guidance for protection of classified information and personnel security per references (a) through (e). This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. NAVPERSCOMINST 5510.1A.

3. Objective. To ensure maximum uniformity and effectiveness in the application of information, industrial, physical, communications, and personnel security program policies by NAVPERSCOM personnel.

4. Scope. This instruction supplements references (a) and (b) for Department of the Navy (DON) Information Security Program (ISP) and DON Personnel Security Program (PSP).

5. Action. All Office of the Chief of Naval Operations (OPNAV) (N135), Bureau of Naval Personnel (BUPERS) Millington, Commander, Navy Installations Command Detachment (CNIC DET), and NAVPERSCOM personnel (military, civilian, and contract) shall comply with references (a) through (d) and this instruction. Appendix A is a list of acronyms and descriptions used extensively throughout this instruction.

6. Forms Availability. See appendix B.

ANN C. STEWART
Deputy Commander,
Navy Personnel Command

Distribution:
Electronic only, via NAVPERSCOM Web site
http://www.npc.navy.mil/Audiences/ForInternal

NAVY PERSONNEL COMMAND (NAVPERSCOM) SECURITY PROGRAM

TABLE OF CONTENTS

CHAPTER 5 - CLASSIFICATION MANAGEMENT

CHAPTER 6 - CONTROL OF CLASSIFIED INFORMATION

CHAPTER 7 - SECURITY STORAGE

CHAPTER 8 - TRANSMISSION AND TRANSPORTATION

CHAPTER 8 - TRANSMISSION AND TRANSPORTATION (CONT'D)

CHAPTER 9 - DESTRUCTION OF CLASSIFIED INFORMATION

CHAPTER 10 - EMERGENCY PLANNING

CHAPTER 11 - VISITS AND MEETINGS

CHAPTER 12 - PERSONNEL SECURITY

CHAPTER 13 - BUILDING SECURITY REGULATIONS

CHAPTER 1

GENERAL REGULATIONS AND ORGANIZATION

0101. SCOPE. This instruction establishes command security policies, responsibilities and procedures to ensure that all National Security Information (NSI) classified under authority of Executive Order 12958 is protected from unauthorized disclosure. No individual will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made regarding their loyalty, reliability, and trustworthiness. A Personnel Security Investigation (PSI) is conducted to gather information pertinent to these determinations. In the absence of specific reference to requirements here or other separate directives, provisions of references (a) through (d). apply.

0102. COMMAND RESPONSIBILITY AND AUTHORITY

1. Commander, Navy Personnel Command (COMNAVPERSCOM) is designated to administer the Information Security Plan (ISP) and Personnel Security Program (PSP) for NAVPERSCOM.

2. Assistant Commander, Navy Personnel Command for Business Operations/Comptroller (PERS-5) and Director, Command Support Services Division (PERS-53) will be assisted by NAVPERSCOM, Security Branch (PERS-534), in security administration and in enforcement.

3. NAVPERSCOM (PERS-534) is responsible for formulation, implementation and enforcement of security programs, their effectiveness and compliance with higher authority directives. NAVPERSCOM (PERS-534) is designated as Security Manager and Security Officer per references (a) and (b).

0103. SECURITY MANAGER/OFFICER RESPONSIBILITIES

1. In addition to duties outlined in references (a) and (b), NAVPERSCOM (PERS-534) is responsible for the following:

a. NAVPERSCOM (PERS-534) is the principal advisor on ISP and PSP in the command and is responsible to COMNAVPERSCOM via NAVPERSCOM (PERS-5) and NAVPERSCOM (PERS-53) for management,

formulation, implementation and enforcement of security policies and procedures for protection of classified information.

b. NAVPERSCOM (PERS-534) duties are outlined in references (a) and (b). NAVPERSCOM (PERS-534) is assisted by:

(1) Assistant for Security Awareness (PERS-534C), who is also designated as Command Mail Manager is responsible for:

(a) Establishing and maintaining an active security education program. The Education program will be based on procedures and guidelines per references (a) and (b) and chapter 2 of this instruction;

(b) Conducting required training for orientation, security refresher, and foreign travel briefings;

(c) Coordinating, scheduling, and setting up the annual security awareness training that is conducted by the Security Manager; and coordinating the annual counterespionage briefing for all personnel having access to information classified Secret or above.

(2) Personnel Security (PERS-534D), who is also designated as Top Secret Control Officer and North American Treaty Organization (NATO) Control Officer, is responsible for:

(a) Classified information control per reference (a);

(b) Processing of NAVPERSCOM personnel (military, and civilian) security investigations and the processing of investigations for public trust positions for contract personnel per reference (b);

(c) NATO briefing, debriefing, and information control per reference (a);

(d) Maintaining the ISP per DoD 5220.22-M of February 2006, Department of Defense (DoD) Industrial Security Manual for Safeguarding Classified Information;

(e) Maintaining list of position sensitivity and Automated Information Systems (AIS) (now called Information

Technology (IT)) designation per DoD 5200.2-R, of January 1987 and reference (b), chapter 5;

(f) Providing command security check in/out process and building access for NAVPERSCOM personnel;

(g) Processing command visit requests (both incoming and outgoing), process base access requests for incoming visitors;

(h) Verifying personnel security clearances and based on eligibility, has delegated authority to grant military and civilian personnel access to classified information;

(i) Issuing courier cards or courier letters;

(j) Executing security termination statements for individuals terminating active military service or civilian employment; and

(k) Verifying type of security investigation, clearance level, and IT level designation on a System Authorization Access Requests (SAAR).

(3) Electronic Key Management System (EKMS)/Communications Security (COMSEC) Material System (CMS) Custodian (PERS-534H), who is assigned as command EKMS manager and in the absence of the Security Manager, designated as the Assistant Security Manager. The EKMS manager is responsible to the Staff Communications Security Material System Responsibility Officer (SCMSRO) and NAVPERSCOM (PERS-534) for management of the command EKMS/COMSEC account per EKMS-1 and is responsible for inventory of safes and safe combinations.

0104. ASSISTANT COMMANDERS, NAVY PERSONNEL COMMAND (ACNPS) AND SPECIAL ASSISTANTS (SAS), RESPONSIBILITIES

1. Designate, in writing (exhibit 1A), a department security assistant. Security assistants will be the focal point of all ISP and PSP security matters within their areas and are responsible for:

a. Receiving, storing, inventory, reproduction, handling, disposition, and distribution of classified information up to Secret;

b. Maintaining a listing of all personnel (military and civilian) showing the authorized access approved by NAVPERSCOM (PERS-534). Personnel listing must be continually evaluated by the security assistant to ensure personnel are eligible for access to classified information or assignment to sensitive duties. Discrepancies to personnel listing must be coordinated with NAVPERSCOM (PERS-534;

c. Forwarding a NAVPERS 5520/6, Request for Security Access to NAVPERSCOM (PERS-534) for all personnel that need access to classified information; and.

d. Being familiar with National Industrial Security Program (NISP), for contract employees per reference (b), article 8-8.

2. Submit names of each department security assistant (including designated assistants with the specific duties they are authorized to perform) to NAVPERSCOM (PERS-534). This information, in the form of a consolidated list, is issued annually. Necessary deletions/additions must be submitted in writing as they occur.

0105. SECURITY INSPECTIONS AND SECURITY ASSIST VISITS

1. Formal security inspections shall be conducted by NAVPERSCOM (PERS-534) once every 3 years per Inspector General (IG) inspection schedule and results identified using reference (a), (exhibit 2C), and reference (b), appendix D.

2. Security assist visits will be conducted by NAVPERSCOM (PERS-534) upon request by any ACNP, or SA. Security assist visits will be accomplished in an informal manner. An informal report will be completed at the conclusion of assist visit and forwarded to requesting ACNP, or SA.

0106. SECURITY SERVICING AGREEMENTS (SSAS). NAVPERSCOM (PERS-534) will have in writing SSAs when specified security functions may be performed for other commands. These SSAs will be agreements as appropriate for security functions being performed (e.g., INFOSEC, personnel, and physical).

SECURITY ASSISTANT DESIGNATION LETTER

From: ACNP/Special Assistant (PERS-Code)
To: Individual Appointed (Full name, Rank/Rate)

Subj: DESIGNATION AS DEPARTMENT SECURITY ASSISTANT

Ref: (a) NAVPERSCOMINST 5510.1B
(b) SECNAV M-5510.36 of Jun 06
(c) SECNAV M-5510.30 of Jun 06

1. Per reference (a), you are appointed as Department Security Assistant for NAVPERSCOM (PERS-Code). Your period of appointment will be from _____ until _____. You will be notified of any change in this appointment.

2. You will be required to become thoroughly familiar with references (a), (b), and (c) as applied to your department.

3. For effective management of the program, you shall:

a. Serve as the department head's advisor and direct representative in matters pertaining to security, and serve as communications link between your department and NAVPERSCOM (PERS-534);

b. Develop written department security procedures, including an emergency plan. These procedures should be consistent with reference (a), chapter 10;

c. Coordinate and implement a security education program within your department;

d. Ensure that threats to security, compromise and other security violations are promptly reported to NAVPERSCOM (PERS-534);

e. Ensure your department's compliance with accounting and control of classified information including receipt, distribution, inventory, reproduction, and disposition;

EXHIBIT 1A

Subj: DESIGNATION AS DEPARTMENT SECURITY ASSISTANT

f. Forward visit clearance requests to NAVPERSCOM (PERS-534) within 30 days of visit;

g. Ensure requests for carrying classified information outside the command are forwarded to NAVPERSCOM (PERS-534) for authorization;

h. Ensure required protection is taken to prevent unauthorized disclosure of classified information to include meetings, carrying classified information, or casual discussion;

i. Ensure you have an inventory of all GSA approved security containers (safes) within department and a list of primary personnel responsible; and

j. Ensure combinations to all security containers will be safeguarded. A SF 700, Security Container Information, will be completed with part 2 stored in a security container in NAVPERSCOM (PERS-534). A SF 702, Security Container Check Sheet, will be kept with each safe showing when opened, closed, and checked. A OPNAV 5510/21, Security Container Records Form, must be in all security containers and a SF 701, Activity Security Checklist, must be used to ensure daily checks for security containers are accomplished.

SIGNATURE
(Title, PERS-Code)

Copy to:
NAVPERSCOM (PERS-534)
(Individual service record or official personnel file)

EXHIBIT 1A (CONT'D)

CHAPTER 2

SECURITY AWARENESS AND EDUCATION

0201. GENERAL. To establish policy, provide guidance, and set forth uniform standards for security education and training program. Security education program shall ensure that all personnel understand the need and procedures for protecting classified information.

0202. SCOPE

a. The success of ISP and PSP is dependent on a vigorous security education and training program. COMNAVPERSCOM places strong emphasis on and promotes a continuing security education program within the command which increases effectiveness of security regulations and directives, instills security awareness in all personnel, and ensures a uniform interpretation and application of security standards. Security education applies to all personnel entrusted to protect classified information or has access to DON information systems.

b. NAVPERSCOM (PERS-534) is required to provide security education and training to all personnel having access to classified information or DON information systems. Some primary tools available to educate personnel are indoctrination, General Military Training (GMT), On-the-Job Training (OJT), command security personnel, and internet. Effective use of these tools will ensure all personnel understand the need and procedures for protecting classified information and DON information systems. The goal is to develop fundamental security habits as a natural element of each task.

0203. RESPONSIBILITIES. Supervisors, in coordination with NAVPERSCOM (PERS-534), are responsible for determining security requirements for their functions and ensuring personnel under their supervision understand security requirements for their particular assignment. OJT is an essential part of command security education and supervisors must ensure that such training is provided. Department security assistants and NAVPERSCOM (PERS-534) will assist supervisors with this training. NAVPERSCOM (PERS-534) is responsible for planning, implementing, enforcing, and supervising the security education and training program of the command.

0204. SECURITY TRAINING REQUIREMENTS

1. Following requirements will be standard for all command personnel:

a. All personnel will receive orientation upon checking onboard in basic principles of security and information systems.

b. All personnel assigned to duties involving classified information will be immediately given a command security orientation brief.

c. All personnel will receive continuous security awareness OJT and GMT by their supervisors, department security assistants and Information Assurance Managers (IAM).

d. Annual security refresher and counterintelligence briefings will be given to all personnel having authorized access to classified information.

2. Training

a. Orientation. Through indoctrination all personnel will know the following:

(1) Certain information, essential to national security, requires protection from disclosure to unauthorized persons;

(2) Classified information will be marked to show level of classification;

(3) Only those who have been officially and specifically authorized may have access to classified information;

(4) Personnel will be continually evaluated regarding their eligibility to access classified information and to be assigned to a sensitive position;

(5) Classified information must be stored, destroyed and protected during transfer from one area to another (including electronic transfer) per reference (a);

(6) Any compromise or other security violation must be reported to NAVPERSCOM (PERS-534);

(7) Any attempt by an unauthorized person, regardless of nationality, to solicit classified information must be reported;

(8) Command security structure (i.e., command security manager, top secret control officer, special security representative, IAM, department security assistant, etc.);

(9) Any special security precautions within the command, (i.e., restrictions on access to spaces or to certain equipment);

(10) Command security procedures for badging, security checkpoints, destruction of classified information, visitors, INFOSEC, command Local Area Network (LAN), etc.;

(11) Their obligation to report suspected security violations or INFOSEC violations; and

(12) Their obligation to report information that could impact on security clearance eligibility of an individual who has access to classified information.

b. OJT. OJT is the phase of security education when security and information systems procedures for assigned position are learned. Supervision of OJT process is critical. Supervisors are ultimately responsible for procedural violations or for compromises that result from improperly trained personnel. Expecting subordinates to learn proper security and information systems procedures by trial and error is not acceptable. OJT shall be a daily practice at NAVPERSCOM.

c. GMT. Protection of classified information and information systems security GMT will be mandatory for all personnel. Department security assistants and department training officers will coordinate this training with NAVPERSCOM (PERS-534).

d. Intranet. NAVPERSCOM (PERS-534) will maintain a Web site on the intranet providing all hands with available training opportunities, current command security, and information systems policy and guidance.

3. Briefings

a. Refresher briefings. Refresher briefings will cover:

(1) New security policies and procedures and continuous evaluation;

(2) Counterintelligence reminders regarding reporting contacts and exploitation attempts and foreign travel issue; and

(3) Command specific security concerns or problem areas. Results of self-inspections, inspector reports, or security violation investigations that provide valuable information for use in identifying command weaknesses.

b. Counterintelligence briefings. These briefings will be coordinated with the local Naval Criminal Investigative Service (NAVCRIMINVSVC) and will contain updated information pertaining to foreign intelligence activities attempting to obtain classified information and will advise personnel of penalties for engaging in espionage activities.

c. Special briefings. Special briefings will be required for the following circumstances:

(1) Foreign travel briefing. Foreign travel briefings will be conducted by NAVPERSCOM (PERS-534). Briefings are to be given to all NAVPERSCOM personnel traveling overseas on official business. For NAVPERSCOM personnel transferring overseas the briefing will also be provided to family members over the age of 14. Upon return of the traveler, they will report any incident - no matter how insignificant it may have seemed - that could have security implications.

(2) New requirement briefing. Whenever security policies or procedures change, personnel whose duties would be impacted by these changes must be briefed as soon as possible.

(3) Program briefings. Briefings that are specified or required by other program regulations (e.g., NATO, Single Integrated Operation Plan - Extremely Sensitive Information (SIOP-ESI), Sensitive Compartmented Information (SCI), etc.)

4. Debriefings

a. A debriefing will be given to all personnel who no longer require access to classified information as a result of;

(1) Transfers from one command to another;

(2) Terminating active military service or civilian employment;

(3) Temporarily separating for a period of 60 days or more, including sabbaticals, leave without pay status, or transferred to Inactive Ready Reserves (IRR);

(4) Expiration of a Limited Access Authorization (LAA);

(5) Inadvertent substantive accesses to information that the individual is not eligible to receive;

(6) Security clearance eligibility revocation; and

(7) Administrative withdrawal or suspension of security clearance and SCI access eligibility for cause.

b. Debriefings will include all classified information in the possession of individual being returned and a complete review of SF 312, Classified Information Nondisclosure Agreement and Espionage Act, including penalties for disclosure. The individual must report to NAVCRIMINVSVC (or to the Federal Bureau of Investigations (FBI) or nearest DoD component) without delay, any attempt by an unauthorized person to solicit classified information.

5. Security Termination Statements. Every security debrief (except when a person is transferring from one command to another) an OPNAV 5511/14, Security Termination Statement, is required. Individuals must read and execute this statement at the time of debriefing. A witness to the person's signature must sign the statement.

6. Duties and Responsibilities

a. NAVPERSCOM (PERS-534) manages the security education and training plan and reports directly to COMNAVPERSCOM via NAVPERSCOM (PERS-53).

b. Department Heads. Ensure that all department personnel carry out the provisions of this instruction. Provide necessary assistance to department security assistant and department IAM in the execution of their duties.

c. Department Security Assistants. Department security assistants shall be responsible for:

(1) Security training for all personnel and assisting supervisors in OJT of command personnel regarding protection of classified information;

(2) Implementing a department security awareness training plan that will include monthly GMT for all personnel; and

(3) Coordinating with NAVPERSCOM (PERS-534) for training requirements.

e. All Hands. Continuously monitor daily practices and habits. Ensure procedures set forth in this instruction are being performed and contact the NAVPERSCOM Security Manager (PERS-534) when there are any questions concerning security. **SECURITY AWARENESS IS AN ALL HANDS EFFORT!**

7. Reports. NAVPERSCOM (PERS-534) will provide COMNAVPERSCOM an annual Security Training Report that includes dates of scheduled training, subject of security training, number of personnel required to attend, and number of personnel required who did not attend.

CHAPTER 3

LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

0301. GENERAL. A loss or compromise exists whenever classified documents, information, or equipment are lost, disclosed to unauthorized persons, subjected to possible compromise, or when regulations for safeguarding such information are violated, whether or not actual loss or compromise occurs.

0302. REPORTING LOSS OR COMPROMISE. Any individual having knowledge of a suspected loss or compromise or unauthorized disclosure of classified information or other violations of security (deliberate or inadvertent) will immediately report the facts to NAVPERSCOM (PERS-534). When a loss or compromise of classified information has occurred NAVPERSCOM (PERS-534) will report loss or compromise to NAVPERSCOM (PERS-53) and NAVCRIMINVSVC.

0303. PRELIMINARY INQUIRY. When report of loss or compromise of classified information has been made, NAVPERSCOM (PERS-534) will submit a draft Preliminary Inquiry Officer (PIO) appointment letter to the NAVPERSCOM Office of Legal Counsel (PERS-00J) to assign a PIO in writing as the command official to conduct a preliminary inquiry per reference (a), chapter 12. The preliminary inquiry will be initiated and completed within 72 hours.

CHAPTER 4

COUNTERINTELLIGENCE MATTERS

0401. MATTERS TO BE REPORTED

1. Basic Policy. Certain matters affecting national security must be reported to NAVCRIMINVSVC so that appropriate counterintelligence action can be taken. All command personnel, whether they have access to classified information or not, will report to NAVPERSCOM (PERS-534) or to the nearest command any activities of sabotage, espionage, international terrorism, or deliberate compromise, involving themselves, their family members, co-workers, or others. Examples of request to be reported include attempts to obtain names, duties, personnel data or characterizations of DON personnel; technical orders, manuals, regulations, base directories, personnel rosters or unit manning tables; and information about designation, strength, mission, combat posture, and development of ships, aircraft, and weapon systems. NAVPERSCOM (PERS-534) will, in turn, notify NAVCRIMINVSVC.

2. Foreign Travel

a. All command personnel possessing a security clearance are required to report to NAVPERSCOM (PERS-534) all personal foreign travel in advance of travel being performed. Supervisors will keep this reporting requirement in mind when they are approving leave for their personnel and ensure individuals report to NAVPERSCOM (PERS-534). Personnel will be reminded of this reporting requirement during orientation security briefings and annual refresher security brief.

b. See chapter 2, paragraph 0204.3.c, for information regarding a foreign travel briefing.

c. When travel patterns (i.e., numerous expensive trips abroad or very frequent travel) or failure to report such travel indicate the need for investigation, NAVPERSCOM (PERS-534) will refer matter to NAVCRIMINVSVC for action.

3. All personnel who possess a security clearance are to report to NAVPERSCOM (PERS-534) any form of contact with any individual, regardless of nationality, whether within or outside scope of individual's official activities in which illegal or unauthorized

access is sought to classified or otherwise sensitive information. Personnel must report if they are concerned that they may be targets of exploitation. NAVPERSCOM (PERS-534) will review and evaluate the information and promptly report to NAVCRIMINVSVC.

0402. LIAISON WITH INVESTIGATIVE AGENCIES. In all matters pertaining to processing security investigations or other investigations, NAVPERSCOM (PERS-534) will maintain official liaison with NAVCRIMINVSVC. All inquiries and visits by representatives of law enforcement or investigative agencies will be referred to NAVPERSCOM (PERS-534) and NAVPERSCOM (PERS-00J) prior to making any disclosures.

0403. SUICIDE OR ATTEMPTED SUICIDE. When any individual who had access to classified information commits or attempts to commit suicide, individual's department security assistant or supervisor will forward all available information to NAVPERSCOM (PERS-534) for reporting to NAVCRIMINVSVC with an information copy to DON Central Adjudication Facility (CAF). Report will, at a minimum, set forth the nature and extent of classified information to which the individual had access and circumstances surrounding the suicide or attempted suicide.

0404. UNAUTHORIZED ABSENTEES. When any individual who has access to classified information is in an unauthorized absentee status, the individual's department security assistant will notify NAVPERSCOM (PERS-534). Department security assistant will conduct an inquiry to determine if there are any indications from the individual's activities, behavior, or associations that their absence may be inimical to the interests of national security. Results of this inquiry will be submitted to NAVPERSCOM (PERS-534). If the inquiry reveals such indications, NAVPERSCOM (PERS-534) will report all available information to NAVCRIMINVSVC for action.

CHAPTER 5

CLASSIFICATION MANAGEMENT

0501. CLASSIFICATION MANAGEMENT POLICY

1. Executive Order 12958 is the basis for classifying National Security Information (NSI).

2. Information classified by a DON Original Classification Authority (OCA) shall be declassified as soon as it no longer meets standards for classification in the interest of national security.

3. Reference (a), chapter 4, provides detailed summary of classification levels and classification management.

4. BUPERS/NAVPERSCOM are not an OCA.

0502. SECURITY CLASSIFICATION GUIDES. Classification guides are approved personally and in writing by an official with appropriate OCA and cognizance over the information involved.

0503. DOWNGRADING, DECLASSIFICATION, AND UPGRADING. OCAs are only authorized to declassify, downgrade, and upgrade classified information. This is not to be confused with administrative responsibility of a holder of classified information to downgrade or declassify as directed by classification guides or instructions on a document. Further guidelines are provided in reference (a), chapter 4.

0504. MARKING REQUIREMENTS. All classified information handled by NAVPERSCOM shall be clearly marked with appropriate classification level and all required "associated markings" per reference (a), chapter 6.

0505. WARNING NOTICES. Warning notices advise holders of a document of additional protective measures such as restrictions on reproduction, dissemination or extraction. Further guidelines are provided in reference (a), chapter 6.

CHAPTER 6

CONTROL OF CLASSIFIED INFORMATION

0601. GENERAL. NAVPERSCOM (PERS-534) will control dissemination of classified documents and controlled unclassified information originated or received by NAVPERSCOM per reference (a), chapter 8.

0602. ACCESS TO CLASSIFIED INFORMATION

1. Only those individuals (military, civilian, and contractor employees (under a classified contract)) with proper adjudicated security investigation, level of clearance, and need to know have access to classified information in the performance of their duties. No person has access to classified information strictly on their position. If a person requires access to classified information to perform their duties, the department security assistant must send a request to NAVPERSCOM (PERS-534) requesting authorization for access to classified information. When request is received by NAVPERSCOM (PERS-534), it will be reviewed for proper adjudicated security investigation, level of clearance, and if a civilian government employee, the request will be checked for sensitivity code to determine if the civilian position is a non-critical-sensitive or critical-sensitive position. If the civilian is in a non-sensitive position, access to classified information will be denied until position is reclassified to non-critical-sensitive or critical-sensitive by the department.

2. Only personnel (military and civilian) authorized by NAVPERSCOM (PERS-543E) can receive unclassified naval messages via Microsoft Outlook Message Folders. Only personnel with proper clearance and access authorized by NAVPERSCOM (PERS-534) can have access to IT systems processing classified naval messages.

3. The command duty officer is authorized to view messages up to and including Secret in the performance of their duties while only in a watch status. Unless authorized by NAVPERSCOM (PERS-534), this does not authorize the person to handle classified information within their department.

4. Courier cards are not required for hand carrying of classified information within and between NAVPERSCOM buildings.

To hand-carry classified information within NAVPERSCOM, use of a standard form cover sheet for classified document attached to a message in a file folder, envelope, or inside a briefcase to prevent inadvertent disclosure when hand carrying is authorized.

5. When traveling outside of the command, NAVPERSCOM (PERS-534) will provide written authorization to all individuals escorting or hand carrying classified information. This authorization may be the DD 2501, Courier Authorization Card, or included on official travel orders, visit requests, or a courier authorization letter. Any of these written authorizations may be used to identify appropriately cleared DoD military and civilian personnel approved to escort or hand carry classified information (except for SCI and Special Access Programs (SAP)). Reference (a), chapter 9, paragraphs 9-12 and 9-13 provide additional provisions for authorization to escort or hand carry classified information.

0603. CLASSIFIED INFORMATION CONTROL. Accountability and control of classified information, and other accountable documents begins with their origin or receipt at the command. NAVPERSCOM (PERS-534) is the central control point and is responsible for overall control of Secret and Confidential information within NAVPERSCOM. NAVPERSCOM (PERS-534) controls all Top Secret information originated and received by the command.

0604. ACCOUNTABILITY AND CONTROL

1. All Top Secret and Secret **(NOT SECRET MESSAGES)** information are recorded by NAVPERSCOM (PERS-534). Top Secret and Secret information received directly by an individual in NAVPERSCOM from any source must be immediately delivered to NAVPERSCOM (PERS-534). Accountability and control of all information by department security assistants, unless specifically exempted by NAVPERSCOM (PERS-534), is as follows:

a. Top Secret Information

(1) Dissemination of Top Secret information within NAVPERSCOM is strictly controlled by NAVPERSCOM (PERS-534) and limited to persons possessing a Top Secret clearance, authorized access and "need-to-know." Top Secret information will be accounted for from time of receipt until destroyed at all times per reference (a).

(2) Top Secret information received from sources other than NAVPERSCOM (PERS-534) must be immediately delivered to NAVPERSCOM (PERS-534) for proper accountability.

(3) An OPNAV 5511/13, Record of Disclosure, will be completed listing all personnel viewing Top Secret information. A SF 703, Top Secret Cover Sheet, will be attached to cover each Top Secret document and a OPNAV 5216/10, Correspondence/Material Control Sheet, attached to the document for material control. When Top Secret information is checked out and removed from NAVPERSCOM (PERS-534) office spaces the OPNAV 5216/10 will document the routing.

(4) Top Secret information must be returned to NAVPERSCOM (PERS-534) prior to 1500 daily. Exceptions to this requirement may only be made by NAVPERSCOM (PERS-534), only if essential, and only if approved storage is available.

(5) When Top Secret information is to be prepared, NAVPERSCOM (PERS-534) must be contacted prior to commencing. NAVPERSCOM (PERS-534) will provide an OPNAV 5216/10, SF 703, OPNAV 5511/13, and a residue envelope. NAVPERSCOM (PERS-534) will assign a Top Secret accountability number. All rough drafts, diskettes, etc., must be placed in the residue envelope and returned to NAVPERSCOM (PERS-534) along with smooth copies. Numbering and marking of Top Secret information is per reference (a).

(6) Top Secret information will not be reproduced without direct approval of NAVPERSCOM (PERS-534).

(7) Destruction of Top Secret information is the exclusive responsibility of NAVPERSCOM (PERS-534). Accordingly, all Top Secret information to be destroyed must be delivered to NAVPERSCOM (PERS-534).

b. Secret Information

(1) Internal transmission and chain of custody of official record Secret information is accomplished by NAVPERSCOM (PERS-534) under a continuous hand-to-hand receipt. Secret documents will only be released to persons having the required access. Documents to be transferred from one office to another will always be routed

via NAVPERSCOM (PERS-534). No department security assistant to department security assistant transfers are permitted.

(2) Department security assistants will establish an inner department system of control for Secret information, which will provide a continuous chain of receipts clearly traceable to the holder of the information. An SF 704, Secret Cover Sheet, is used to cover each Secret document and an OPNAV 5216/10 must be attached to the document.

(3) When Secret information is originated for transmission, it will be prepared for transmission per reference (a), chapter 9.

(4) When directed by NAVPERSCOM (PERS-534), departments must submit an inventory of Secret documents on hand, based on a physical examination of each document. This inventory is balanced against NAVPERSCOM (PERS-534's) record of official custody. Discrepancies which cannot be resolved by the department involved will be referred to NAVPERSCOM (PERS-534).

c. Confidential Information. An SF 705, Confidential Cover Sheet, and an OPNAV 5216/10 are affixed to all Confidential information received (except messages) by NAVPERSCOM (PERS-534) prior to routing. Departments receiving Confidential information will provide security protection for all Confidential information received, originated, transmitted or stored to the extent required by this instruction.

2. Classified Messages. Top Secret messages are handled in the same manner described above for Top Secret information. All NATO messages received by the command will be handled by NAVPERSCOM (PERS-534). The receiving office code is responsible for handling, distributing, and disposing of incoming Secret and Confidential messages. Identification markings of a message are the word Secret or Confidential at the head and foot of each page of the message. Generally, size and color of this marking is same as the text. Secret and Confidential messages received from NAVPERSCOM Message Center is not controlled by NAVPERSCOM (PERS-534). It is the responsibility of the department security assistant receiving messages to examine each one carefully and affix a Secret or Confidential Material Control Record and a Secret or Confidential Cover Sheet appropriately.

a. All classified message traffic (Secret and Confidential) to BUPERS/NAVPERSCOM will be received and processed via the Navy Marine Corps Internet (NMCI) Secret Internet Protocol Router Network (SIPRNET). Only personnel that have been authorized by NAVPERSCOM (PERS-534) will be granted access to classified IT systems.

3. Naval Warfare and Tactical Publications

a. Any NAVPERSCOM employee who has appropriate clearance may check out Naval Warfare and Tactical Publications from their department security assistant. Classified publications must be stored in appropriate authorized security containers for the level of classification when not being used. NAVPERSCOM (PERS-534) will distribute publications once received to appropriate department security assistants when received. Department security assistants must maintain control of classified publications and allow only those individuals with proper security clearance and need-to-know to view contents. Publications may not be checked out on a permanent retention basis and are subject to recall by NAVPERSCOM (PERS-534). Publications will be returned to NAVPERSCOM (PERS-534) when no longer needed by the department.

b. All information in these publications, regardless of classification, is considered privileged information and, if unclassified, is to be treated as For Official Use Only (FOUO). The person who has drawn one of these publications is personally responsible for accountability, safeguarding, and maintenance of the publication, in the same manner as other classified information.

0605. COPYING CLASSIFIED DOCUMENTS

1. Department security assistants must ensure that all copy (e.g., Ricoh, etc.) and facsimile machines are identified as to what classification is authorized within their PERS-code.

2. Top Secret documents will not be detached from routing sheets or duplicated without proper approval from NAVPERSCOM (PERS-534). Information originating outside of DoD will not be reproduced without consent of originating agency.

3. Each ACNPC or SA will institute strict procedures to ensure copying of classified information within their department is

absolutely essential and limited to exact quantities for the task involved. No Top Secret or Secret information will be copied without NAVPERSCOM (PERS-534) approval.

4. Destruction of classified information will be per reference (a), chapter 10.

5. Reproduced copies of classified documents, as well as waste, samples, etc., will be controlled in the same manner as the original document.

6. Copies, reproduced using typical office copiers, can leave legible images on plastic surfaces. These images can transfer to plastic binders or plastic document protectors after lengthy contact. Classified document cover sheets will be used to preclude transferring classified image to plastic materials.

0606. HANDLING PRECAUTIONS AND OFFICE PRACTICES

1. Following precautions will be observed by NAVPERSCOM personnel to prevent deliberate or casual access to classified information by unauthorized persons:

a. Keep classified documents stored per reference (a), chapter 10.

b. If it is necessary to vacate the office, all classified information must be returned to its stowage container and locked, or left in the custody of persons cleared for access to subject matter.

c. Receive visitors in areas devoid of classified information whenever possible, unless the purpose of the visit is to discuss such information.

d. Protect all working information containing classified information, e.g., rough drafts, stencils, stenographic notes, and papers, in the same manner as original classified documents, until no longer required and destroyed.

e. Do not discuss classified information over any unsecured telephone or internal communications systems.

f. Immediately report any loss, compromise, or suspected compromise to NAVPERSCOM (PERS-534). During non-working hours, report any loss to NAVPERSCOM Duty Officer. For classified documents lost while in a travel status where no U.S. military activity exists in the area, notify nearest NAVCRIMINVSVC or FBI field office, as well as NAVPERSCOM (PERS-534), by the quickest means possible.

0607. CONTROL OF CLASSIFIED WORKING PAPERS OR PRELIMINARY DRAFTS

1. The terms (classified working papers or preliminary draft) include, but are not limited to, the following: All written information whether handwritten, printed, or typed; rejected copies; magnetic recordings; all photographs, negatives, exposed or printed films; all punched cards or tapes, etc., developed in connection with the handling, processing, production, and utilization of classified information. Working papers containing classified information will be:

a. Dated when created;

b. Marked on each page with the highest classification of any information contained in the document;

c. Protected following classification assigned; and

d. Destroyed when they have served their purpose. Classified notes from a training course or conference are considered working papers.

2. Top Secret working papers will be prepared, controlled, and accounted for in the same manner as the finished document. Also, working papers meeting the following description should be controlled as if they were finished documents.

a. Working papers released by the originator outside NAVPERSCOM, transmitted electronically, or transmitted through message channels within NAVPERSCOM.

b. Retained more than 90 days from date of origin.

c. Filed permanently.

0608. NORTH ATLANTIC TREATY ORGANIZATION (NATO) MATERIAL

1. DON documents incorporating NATO information must be marked per reference (a).

2. All personnel requiring access to NATO must first be cleared for access to an equivalent level of classified information. Personnel who are to have access to NATO information must be aware of the appropriate NATO security regulations and the consequences of negligence. The NATO Control Officer will brief all personnel requiring access to NATO and complete an OPNAV 5511/27, Briefing/Re-briefing/Debriefing Certificate, to certify briefing. A completed OPNAV 5511/27 will be retained by NAVPERSCOM (PERS-534).

CHAPTER 7

SECURITY STORAGE

0701. SECURITY CONTAINER CUSTODIAN. Department security assistants from each department must ensure security containers located within their spaces have a principal custodian and an alternate designated for each security container. This designation is indicated on a SF 700, Security Container Information, affixed to inside of the drawer containing combination lock. Custodians and other persons listed on a SF 700 must possess a security clearance and access equal to or higher than classification level of information stowed in container. Principal custodian bears primary responsibility for compliance with security procedures for container and its contents per reference (a), chapter 10.

0702. COMBINATIONS

1. Combinations for security containers will be changed per reference (a), chapter 10.

2. Only individuals with proper clearance and access equal to or higher than classification level of information in container and a need to know will change combinations. NAVPERSCOM (PERS-534) personnel will change any combination or assist office code in changing their security container combinations. Once combination has been changed, a SF 700, parts 2 and 2A will be given to NAVPERSCOM (PERS-534) for storage in security container located in NAVPERSCOM (PERS-534).

NOTE: When combinations are recorded, such records will be marked with highest classification level being protected.

0703. CLASSIFIED INFORMATION STORAGE. When not in actual use or under immediate surveillance of an authorized person, classified information will be secured and stored per reference (a), chapter 10.

0704. CLASSIFIED STORAGE EQUIPMENT. Standards for classified storage equipment will be per reference (a), chapter 10.

0705. LOCKING PROCEDURES. Security containers will be locked and secured per reference (a), chapter 10.

0706. DAILY SECURITY INSPECTION

1. All NAVPERSCOM codes handling classified information will establish a double-check system to ensure that at the end of each working day:

a. All classified information is properly stowed in authorized security containers;

b. No classified information is left in or on desks, tables, files, etc.;

c. Contents of wastebaskets should be checked to ensure they contain no classified information;

d. Classified shorthand notes, computer disks/compact disks (CDs), rough drafts, and similar papers have been properly stowed;

e. Desk blotters, computer disks/CDs are protected in the same manner as required for highest level of classification for which they have been used; and

f. Security containers that contain classified information are locked and properly secured. A record of above assignments and inspections will be maintained using an SF 701, Activity Security Checklist, in each office handling classified information. A SF 702, Security Container Check Sheet, must be prominently posted on each security container.

CHAPTER 8

TRANSMISSION AND TRANSPORTATION

0801. GENERAL

1. Transmission and transportation of classified information will be per reference (a), chapter 9.

a. Individuals who have proper clearance, access and need-to-know, may hand carry classified information within the command and between buildings as part of their normal duties. Individuals will use a cover sheet, file folder/briefcase to prevent inadvertent disclosure of classified information when movement is from one building to another, or in an elevator, or through public areas. If movement requires transportation other than walking, classified information will be double wrapped. A briefcase may be considered as the outer wrapping.

b. Personnel hand carrying classified information outside the command will obtain courier authorization in writing from NAVPERSCOM (PERS-534) prior to removing the classified information. Courier authorization may be in the form of a letter or a DD 2501, Courier Authorization Card, issued by NAVPERSCOM (PERS-534). Personnel discovered carrying classified information without written authorization will be detained until NAVPERSCOM (PERS-534) is notified and takes charge of the situation. Exhibit 8A will be used to request authorization to transport classified information. If transporting classified information via commercial passenger aircraft and a letter requesting authorization is required, employees must have an authorized courier letter or a DD 2501 signed by NAVPERSCOM (PERS-534) (exhibit 8B).

c. Following conditions will be met if classified information needs to be transported outside the command:

(1) A determination is made that necessary classified information is not available at the activity involved.

(2) Time does not permit information to be transmitted by normal channels.

(3) Appropriate correspondence, serialized and dated, is prepared and processed through NAVPERSCOM (PERS-534). Confidential information need not be processed through NAVPERSCOM (PERS-534) but must meet all other requirements for Secret. (Note: When classified information is not transported beyond the boundary of the command and is removed for temporary use, classified information must be returned to NAVPERSCOM (PERS-534) custody within the same day. If classified information is being removed from the command, all other provisions of this chapter will apply.) When classified information is removed under these conditions, department security assistant must maintain a list of information being carried and an accounting conducted immediately upon return by the custodian. Any discrepancies, including loss/possible compromise must be reported immediately to NAVPERSCOM (PERS-534).

(4) Classified information must not be opened, read, studied, displayed, or used in any manner in public places, or conveyances.

(5) When classified information is carried in a private, public, or government conveyance, it will not be stowed in any detachable storage compartment such as trailers, luggage racks, etc.

(6) Classified information must be in physical possession of the individual at all times if proper storage at a U.S. Government activity or appropriately cleared contractor facility is not available. Classified information will not be left in such places as locked automobiles, hotel rooms, hotel safes, train compartments, private residences, public lockers, etc.

(7) When return of classified information is required, the traveler will request the activity to return information via appropriate authorized channels per reference (a). If the activity retains Secret information, the traveler is required to obtain a receipt, which is delivered to NAVPERSCOM (PERS-534).

0802. TRANSMISSION AND RECEIPT OF CLASSIFIED INFORMATION

1. Transmission of classified information will be per reference (a), chapter 9.

2. Receipt System

a. Top Secret information is transmitted under a continuous chain of custody.

b. A receipt between commands and other authorized addresses covers Secret information. Failure to sign and return a receipt to sender may result in a report of possible compromise.

c. Receipts for Confidential information are not required except when transmitted to a foreign government (including embassies in the U.S.).

d. Sender of information will attach receipt to the inner cover. A postcard receipt form, such as an OPNAV 5510/10, Record of Receipt, may be used for this purpose. Receipt forms will be unclassified and contain only information necessary to identify information being transmitted. Receipts will be retained for at least 2 years.

e. In those instances where a flyleaf (page check) form to be returned to the sender is used with classified publications, another receipt is not needed.

0803. ELECTRONIC TRANSMISSION OF CLASSIFIED INFORMATION

1. Secure Telephone Equipment (STE) is a telephone unit providing reliable, low cost secure voice and data capability for conducting official business involving classified information. To permit access to a STE, the individual must be eligible for access to classified information at the Secret level.

2. Authorized Classified Facsimile. The classified secure facsimile system located in the security office; building 769, room 184, is authorized for classified transmission. The secure facsimile may be reached during the workweek from 0700 to 1600 commercial (901) 874-2657/DSN 882. Secure facsimile system is TEMPEST approved and is authorized for transmission of information classified Top Secret and below. Highly sensitive documents may also be transmitted on the secure facsimile.

0804. PROCESSING CLASSIFIED INFORMATION ON NAVPERSCOM COMPUTERS. Classified information will not be processed on any command IT without the direct approval of NAVPERSCOM (PERS-534). NAVPERSCOM

personnel requiring access to classified NMCI SIPRNET systems must forward a SAAR, to NAVPERSCOM (PERS-534) via their supervisor. Once NAVPERSCOM (PERS-534) receives the SAAR, NAVPERSCOM (PERS-534) will verify to see if the person requesting access has the appropriate security clearance eligibility and access authorization.

5510
Ser XXX/
Date

From: Commander, Navy Personnel Command

Subj: AUTHORIZATION TO TRANSPORT CLASSIFIED INFORMATION

Ref: (a) SECNAV M-5510.36, Chapter 9
(b) NAVPERSCOMINST 5510.1B

1. Per references (a) and (b), the below individual has authorization to transport classified information.

a. The full name, rank/grade, and command name.

b. Description of the personal identification the individual will present (e.g., State Drivers License Number or Government Identification Card).

c. Description of the material being carried (e.g., three sealed packages, 9" X 8" X 24"), addressee and sender.

d. The point of departure itinerary, destination, and known transfer points.

e. A date of issue and expiration date.

f. NAVPERSCOM Security Manager's (name, title, and signature) shall be on the face of each package or carton.

g. NAVPERSCOM Command Duty Officer telephone number is (901) 874-3071/DSN 882.

2. If a return trip is necessary, the host security official at the original destination shall conduct all necessary coordination and provide an endorsement to the original courier authorization letter to include the updated itinerary.

EXHIBIT 8A

Subj: AUTHORIZATION TO TRANSPORT CLASSIFIED INFORMATION REQUEST

3. Confirmation of this authorization may be obtained by calling NAVPERSCOM Security Manager (PERS-534) at (901) 874-3091/DSN 882.

NAME (NAVPERSCOM Security Manager)
By direction

EXHIBIT 8A (CONT'D)

5510
Ser 534/
Date

From: Commander, Navy Personnel Command

Subj: AUTHORIZATION TO HAND CARRY CLASSIFIED INFORMATION ABOARD COMMERCIAL PASSENGER AIRCRAFT

Ref: (a) SECNAV M-5510.36, Chapter 9
(b) NAVPERSCOMINST 5510.1B

1. Per references (a) and (b), the below individual has authorization to transport classified information.

a. The full name, rank/grade, and command name.

b. Description of the personal identification the individual will present (e.g., State Drivers License Number or Government Identification Card).

c. Description of the material being carried (e.g., three sealed packages, 9" X 8" X 24"), addressee and sender.

d. The point of departure itinerary, destination, and known transfer points.

e. A date of issue and expiration date.

f. NAVPERSCOM Security Manager's name, title, and signature shall be on the face of each package or carton.

g. NAVPERSCOM Command Duty Officer telephone number is (901) 874-3071/DSN 882.

2. If a return trip is necessary, the host security official at the original destination shall conduct all necessary coordination and provide an endorsement to the original courier authorization letter to include the updated itinerary.

EXHIBIT 8B

Subj: AUTHORIZATION TO HAND CARRY CLASSIFIED INFORMATION ABOARD COMMERCIAL PASSENGER AIRCRAFT

3. Confirmation of this authorization may be obtained by calling NAVPERSCOM Security Manager (PERS-534) at (901) 874-3091/DSN 882.

NAME (NAVPERSCOM Security Manager)
By direction

EXHIBIT 8B (CONT'D)

CHAPTER 9

DESTRUCTION OF CLASSIFIED INFORMATION

0901. GENERAL. Destruction of information classified will be per reference (a), chapter 10. Secret and below classified information will be destroyed using authorized shredders located in NAVPERSCOM buildings 453, 457, 768, 769, and 791. All Top Secret information will be returned to NAVPERSCOM (PERS-534), building 769, room 184 for destruction by NAVPERSCOM Top Secret Control Officer.

0902. DESTRUCTION REPORTS

1. A record of destruction is required for Top Secret information. Use of an OPNAV 5511/12, Classified Material Destruction Report, is no longer required. Record destruction of Top Secret and any special types of classified information (if required) by any means as long as the record includes complete identification of information destroyed and date of destruction. Two witnesses who have authorized access to the information being destroyed shall execute the record of destruction. Retain Top Secret records of destruction for 5 years. Records of destruction are not required for waste products containing Top Secret information.

2. Records of destruction are not required for Secret and Confidential information except for special types of classified information per reference (a), chapters 7 and 10.

CHAPTER 10

EMERGENCY PLANNING

1001. GENERAL

1. Emergencies can be categorized as accidental or hostile. Natural disasters such as fire or flood are examples of accidental emergencies whereas enemy attack or civil uprising would be defined as hostile actions. In an accidental emergency, action must be directed toward maintaining continuous control and accountability of all classified and privileged information. During hostile action, it must be assumed that information itself is a target and all actions must be directed toward preventing a compromise.

2. When confronting an emergency situation, three basic alternatives are available;

a. Secure the information;

b. Remove the information; and

c. Destroy the information.

3. Execution of any of these alternatives is in such a manner as to minimize the risk of loss of life or injury to personnel.

1002. SECURE THE INFORMATION. In case of either an accidental or hostile emergency, securing information is the primary means of protecting NAVPERSCOM classified and privileged information. All personnel having custody of such information will immediately store the information in its authorized container, being certain to securely lock the container. Upon return to the area, all containers will be inventoried immediately and results reported to department security assistant. Discrepancies will be brought to the immediate attention of the cognizant ACNPC/SA, and NAVPERSCOM (PERS-534).

1003. REMOVE THE INFORMATION

1. Because of the nature of the mission of NAVPERSCOM, removal of all classified and privileged information is the least likely emergency action to be taken. Local contingency planning does not

envision evacuation of the area except in the most severe circumstances, which would necessarily entail emergency destruction of all classified information. In the unlikely event that removal of information is ordered, only the most sensitive information should be removed. Classified information must be transported in a government vehicle and the courier must be directed to maintain continuous accountability.

2. All CMS information will be removed and relocated to the COMSEC vault in building 769, room 184 if time permits. EKMS Manager/COMSEC custodian must be contacted prior to removal of any COMSEC information or equipment.

1004. DESTROY THE INFORMATION

1. Each department security assistant will be directed to implement department emergency destruction plan upon notification to commence emergency destruction of classified and privileged information. Importance of beginning destruction sufficiently early to prevent loss of information cannot be overemphasized. Effects of premature destruction are considered relatively inconsequential when measured against the possibility of compromise.

2. Priorities for emergency destruction are as follows:

a. Priority One. Information, which, if captured, would cause exceptionally grave damage (Top Secret).

b. Priority Two. Information, which if captured, would cause serious damage (Secret).

c. Priority Three. Information, which if captured, would cause identifiable damage (Confidential).

3. "Priority One" and all COMSEC information will be returned to building 769, room 184 for destruction when possible.

1005. IMPLEMENTING AUTHORITY

1. COMNAVPERSCOM will be implementing authority for any emergency actions; however, the senior individual present in a space containing classified and privileged information may implement

emergency procedures and deviate from established plans if urgency of the situation precludes awaiting emergency instructions.

2. Per EKMS-1, the EKMS Manager/COMSEC custodian with authorization from COMNAVPERSCOM is the only person authorized to initiate COMSEC information emergency destruction.

CHAPTER 11

VISITS AND MEETINGS

1101. GENERAL. For security purposes, the term visitor applies to any person who is not attached to or employed by NAVPERSCOM or a person on Temporary Additional Duty (TEMADD) is considered a visitor. Personnel on Temporary Duty (TEMDU) orders or those personnel assigned on a quota to a school for a course of instruction are also considered visitors. Visit access to classified information is specified in reference (b), chapter 11.

1102. INCOMING VISITS. NAVPERSCOM (PERS-534) is the central control point for receiving and recording incoming visit requests from DOD, other government agencies, foreign representatives, and contractor activities and is responsible for confirming all visitor and contractor security clearances when access to classified information will be required. The NAVPERSCOM office to be visited or having cognizance over the contract is responsible for ensuring that visitors or contractors are informed of the necessity of forwarding a visitor request to NAVPERSCOM (PERS-534). Upon receipt of an incoming visit request, NAVPERSCOM (PERS-534) will forward a copy of it to the point of contact for concurrence or nonoccurrence with the proposed visit. If offices to be visited receive a visit request directly, the request must be forwarded to NAVPERSCOM (PERS-534) for recording purposes. All visit requests must be renewed annually. At no time will visitors or contractors be given access to classified information without proper approval from NAVPERSCOM (PERS-534).

1103. OUTGOING VISITS

1. Requests for visits by NAVPERSCOM personnel, which will necessitate their having access to classified information, will be made by using OPNAV 5521/27, Visit Request/Visitor Clearance Data. OPNAV 5521/27 will be filled in by the initiating office, per reference (b), and forwarded to NAVPERSCOM (PERS-534) for security certification and approval. NAVPERSCOM (PERS-534) will enter visit in the Joint Personnel Adjudication System (JPAS) if the Security Management Office (SMO) of visiting command if known. Requests for visits will be submitted in advance of proposed visit and in sufficient time to permit processing. In exceptional cases, the above information may be furnished by telephone, provided such information is confirmed promptly in writing. Under

no circumstances may personnel hand carry their own visit request to the places being visited. When a telephone request is made, an OPNAV 5521/27 is submitted to NAVPERSCOM (PERS-534) prior to arranging the verbal visit request. NAVPERSCOM departments making arrangements for sponsored visits that include personnel from other DoD or contractor agencies should notify those activities to forward security confirmation for their personnel to the activity to be visited.

2. Visit request may be transmitted by the following means:

a. Facsimile machine. Transmission by facsimile must be on official letterhead or an OPNAV 5521/27 visit request and must include all of the required information.

b. Electronically transmitted via e-mail. Visit requests via e-mail must be transmitted from the command security manager to the security manager of the command to be visited. Additionally, procedures must be established to preclude electronic transmission by unauthorized personnel.

1104. VISITS TO CONTRACTOR FACILITIES. When personnel require access to classified information in connection with a visit to a contractor facility, the visit request is submitted per section 1103 above, with one exception. Visit request must include contract or solicitation number. NAVPERSCOM departments submitting a visit request to a contractor facility will forward visit request to NAVPERSCOM (PERS-534) for approval. Under no circumstances are departments to make prior notification or verbal requests for visits. NAVPERSCOM (PERS-534) will assist departments in proper procedures for completing an OPNAV 5521/27.

1105. VISITS BY REPRESENTATIVES OF THE GENERAL ACCOUNTING OFFICE (GAO). Properly cleared and identified representatives of GAO may be granted access to classified DON information in the performance of their assigned duties and responsibilities per reference (b). All GAO visit requests are kept on file in NAVPERSCOM (PERS-534).

1106. VISITS BY FOREIGN NATIONALS. Policy and procedures for visits by foreign nationals are contained in reference (b). To ensure proper coordination and control of foreign disclosure within DON, authority for disclosure of classified information to foreign nationals must be coordinated through NAVPERSCOM (PERS-534).

1107. VISITS TO FOREIGN COUNTRIES. When a DON activity proposes to sponsor an official visit to a foreign country, the sponsoring activity will ensure that nominees are reliable and trustworthy and, if classified information is involved, that they have been properly cleared to handle information of the security classification involved in the visit. If classified DON information is to be discussed with foreign nationals, prior authorization for such discussions must be obtained from Navy International Programs Office (NAVIPO). Further guidelines on this subject are contained in reference (b).

1108. CLASSIFIED MEETINGS

1. Protection of classified information within a conference room is the responsibility of the office sponsoring the conference. All offices conducting meetings should be familiar with the guidelines of reference (a).

a. The office scheduling a conference classified Top Secret in a conference room not guarded by security alarm systems will notify NAVPERSCOM (PERS-534) at least 30 working days in advance, in order that an electronic countermeasure inspection can be scheduled. Upon completion of electronic countermeasure inspection of conference room, it is the responsibility of the office scheduling conference to provide strict access control until conclusion.

b. For conferences or meetings in which information classified Secret or above is to be discussed, the office scheduling conference is responsible to provide a monitor for passageway adjacent to conference room while conference/meeting is in session. Such monitors must have a security clearance/access equivalent to classification of the conference.

c. If any telephones, tape recorders, or other electronic equipment are located in conference rooms, these should be disconnected during classified discussions.

d. The office conducting the conference, briefing, or presentation will make an inspection at conclusion to ensure no classified information remains in the room.

2. If foreign representatives are expected to attend a classified meeting, a command may not accept security sponsorship without

prior approval of OPNAV (N09N). Requests to sponsor meetings involving foreign representatives must be submitted not later than 45 days prior to the meeting date.

CHAPTER 12

PERSONNEL SECURITY

1201. GENERAL

1. No person will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made of their loyalty, reliability, and trustworthiness and the individual has executed a SF 312, Classified Information Nondisclosure Agreement. Initial determination will be based on Personnel Security Investigations (PSI) appropriate to access required or to other considerations of the sensitivity of duties assigned. No individual will be given access to classified information strictly because of their rank. Reference (b) provides guidance governing DON Personnel Security Program (PSP).

2. Only NAVPERSCOM (PERS-534) is authorized to request PSIs for NAVPERSCOM personnel.

3. PSI requirements are contained in reference (b), chapter 6. Only the minimum investigation to satisfy a requirement may be requested.

1202. RESPONSIBILITIES. The granting of access to classified information is a command function. NAVPERSCOM (PERS-534) is authorized, in the name of COMNAVPERSCOM, to grant appropriate security access for NAVPERSCOM personnel.

1203. POSITION SENSITIVITY

1. National security positions in the command that require use of, or access to, classified information under Title 5, Code of Federal Regulations (CFR), 732.201, require positions be assigned a position sensitivity level. Position sensitivity levels are Special Sensitive (SS), Critical Sensitive (CS), and Non-Critical-Sensitive (NCS).

2. Military, civilian, and contract employees performing duties on unclassified IT will be assigned to one of three position sensitivity designations per DoD 5200.2-R, of January 1987, appendix K and reference (b).

3. Security clearances and investigative requirements for military, civilian, and contractor employees are predetermined based on degree of access required and category of sensitivity assigned to criteria for designating IT position category.

4. Military, civilian, and contractor personnel in a non-sensitive billet will not be authorized access to any sensitive or classified information.

1204. REQUIREMENTS FOR ACCESS AND CLEARANCE ELIGIBILITY

1. All civilian and military personnel reporting aboard NAVPERSCOM are required to check-in with NAVPERSCOM (PERS-534) in building 769, room 184.

2. During check-in process, all civilian and military personnel will be informed they do not automatically have access to classified information. For access to classified information, each individual checking aboard must submit a request for access to classified information through their department security assistant. Need for access is evaluated and determined by position sensitivity and need-to-know. If individual is in a SS, CS, or NCS position that requires access to classified information and has need-to-know, the department security assistant must submit a NAVPERS 5520/6, Request for Security Access, to NAVPERSCOM (PERS-534). Eligibility for access to classified information for military and civilian personnel assigned to NAVPERSCOM is certified by NAVPERSCOM (PERS-534). Once determination has been made that individual requires access to classified information and request for security access is received, NAVPERSCOM (PERS-534) will authorize access to view classified information only if DONCAF has determined eligibility and security investigation is current. If investigation is not current, individual will be required to update investigation using the Electronic Personnel Security Questionnaire (e-QIP) or via a SF 86. NAVPERSCOM (PERS-534) can grant interim clearance for access when proper paperwork has been submitted and/or released to Office of Personnel Management (OPM) and Defense Security Service (DSS).

3. All civilian and military personnel checking out and departing NAVPERSCOM must check out with NAVPERSCOM (PERS-534).

1205. CONTINUOUS EVALUATION OF ELIGIBILITY

1. Per reference (b), chapter 10, personnel security responsibilities do not stop once a favorable personnel security determination is made. Any person having knowledge or information that reflects adversely on an individuals loyalty, reliability, and trustworthiness from a security prospective, will immediately report the full particulars and circumstances to NAVPERSCOM (PERS-534) for evaluation/further investigation.

2. Security assistants, command legal staff officials, and particular supervisors are cautioned that information which could place an individual's loyalty, reliability, and trustworthiness in question has to be evaluated from a security perspective and are hereby required to familiarize themselves with the adjudication policy in reference (b). Behavior indicating unexplained affluence, financial instability, alcohol and drug abuse, mental or emotional instability, or criminal conduct is potentially significant to an individual's security status and information concerning these issues must be reported to NAVPERSCOM (PERS-534).

3. Co-workers have an equal obligation to advise their supervisor or NAVPERSCOM (PERS-534) when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

1206. PROOF OF U.S. CITIZENSHIP FOR SECURITY CLEARANCE/ACCESS. Citizenship validation will be accomplished per reference (b), appendix I.

1207. TEMPORARY AND ONE-TIME ACCESS. Circumstances may arise in which temporary and one-time access to classified information is appropriate for personnel otherwise eligible for access involved but who do not currently hold a security clearance at that level, and the assigned duties do not require access. Request should be submitted to NAVPERSCOM (PERS-534) detailing reasons and length of time desired for temporary access. Reference (b), chapter 9, paragraphs 9-6, 9-7, and 9-8 explains one-time and temporary access requirements in detail.

1208. DENIAL OR REVOCATION OF CLEARANCE/ACCESS FOR CAUSE. When a personnel security determination has been made that an individual does not meet or no longer meets criteria for a security

clearance, the clearance will be denied or revoked for cause by DONCAF. Reference (b) provides an extensive explanation of denial or revocation of security clearance for cause process.

1209. SUSPENSION OF ACCESS FOR CAUSE. When questionable or unfavorable information becomes available concerning an individual who has been granted access to classified information procedures in reference (b), chapter 9, paragraph 9-18 apply.

1210. TERMINATING, WITHDRAWING, OR ADJUSTING ACCESS

1. Access to classified information terminates when an individual transfers from the command. The process to terminate, withdraw, or adjust access will be per reference (b), chapter 9, paragraph 9-17. NAVPERSCOM (PERS-534) will debrief individuals per reference (b), chapter 4, paragraph 4-11, but execution of an OPNAV 5511/14 is not required.

2. NAVPERSCOM (PERS-534) will administratively withdraw an individual's access when permanent change in official duties (i.e., rating change) eliminates the requirement for security clearance and access and when the individual separates from DON or otherwise terminates employment. NAVPERSCOM (PERS-534) will debrief individuals as outlined in reference (b), chapter 4, paragraph 4-11 and execute an OPNAV 5511/14, which will be filed in individual's service record or official personnel folder. NAVPERSCOM (PERS-534) will forward an electronic incident report via JPAS to notify DONCAF that the individual no longer requires clearance and access.

3. When level of access required for an individual's official duties change, NAVPERSCOM (PERS-534) will adjust authorized access accordingly, provided new requirement does not exceed level allowed by the security clearance. If level of access required will exceed level allowed by DONCAF security clearance certification, NAVPERSCOM (PERS-534) will request appropriate investigation and may consider interim clearance procedures per reference (b), chapter 8, paragraph 8-5.

1211. SECURITY TERMINATION STATEMENT

1. An OPNAV 5511/14 is obtained from the following personnel prior to their separation:

a. Civilian personnel retiring, resigning from Federal service, or temporarily separating for more than 60 days including sabbaticals and leave without pay.

b. Military personnel being retired, released from active duty, or discharged.

c. When security is revoked for cause see reference (b), chapter 9, paragraph 9-18.

2. NAVPERSCOM (PERS-534) will execute signing of an OPNAV 5511/14 for military and civilian personnel of NAVPERSCOM. All civilian personnel's OPNAV 5511/14 will be filed in individual's official record and military personnel's OPNAV 5511/14 will be forwarded to the Personnel Support Activity Detachment.

1212. CLEARANCE OF PERSONNEL NOT REGULARLY ASSIGNED

1. In connection with disclosure of classified information to persons temporarily assigned (TEMDU, TEMADD, Temporary Active Duty (TEMAC), and temporary Active Duty for Training (ADT)) personnel security clearances/accesses are required and will be granted per the following:

a. TEMADD. Military personnel reporting for TEMADD should be cleared by their CO prior to reporting and their clearance/access status reported to NAVPERSCOM (PERS-534) in writing, either in their orders or by separate correspondence.

b. TEMDU. Military personnel reporting for TEMDU are, in most cases, reporting for briefing or instruction enroute to a new duty station. Such clearance/access should be requested in advance of reporting whenever practicable.

c. Training Duty. Navy Reservists reporting for TEMDU for training must be cleared by their active duty command responsible for their records. The reservist's cognizant organization must specify the degree of clearance/access required for training duty when acting upon the request for such duty. Attach a NAVPERSCOM 5520/6, Request for Security Access.

CHAPTER 13

BUILDING SECURITY REGULATIONS

1301. GENERAL. The term "Building Security" is used to identify regulations issued by DON for protection of building spaces or facilities. These regulations are limited to control of access to building, property removal, and related matters.

1302. SECURITY HOURS. COMNAVPERSCOM sets building security hours. Security hours are when doors are locked. During these hours, the Common Access Card (CAC) must be used for admittance to NAVPERSCOM buildings. The CAC should be conspicuously worn on outer garments while in a NAVPERSCOM building for identification purposes.

1303. BACKGROUND. Per reference (d), a system of personnel identification is a required basic security measure at naval installations and activities. Positive identification provides a means for visually establishing authorization for personnel movement and actions. Personnel requiring access to NAVPERSCOM buildings are to be identified and access controlled during weekends, holidays, and during security hours.

1304. COMMON ACCESS CARD (CAC). All NAVPERSCOM military, civilian, and contractor personnel are required to possess a CAC. Contractor personnel must have on file with NAVPERSCOM (PERS-534) a valid visit request validated by their NAVPERSCOM Trusted Agent (TA)/Contract Client Representative (CCR) point of contact.

1305. ADMITTANCE

1. Personnel requiring access to building Level Two Restricted Spaces must have approved access granted by NAVPERSCOM (PERS-534). A visitor control log will be used in Restricted Spaces to log all personnel and visitors.

2. During normal working hours, anyone having the following un-expired badges: NAVPERSCOM, DoD, or a photographic identification card issued by a U.S. Government agency, including retired military, and military family members, or a valid

identification listed below is authorized access to NAVPERSCOM buildings for official business.

a. Visitors from Other Federal Agencies. Security representatives of the following agencies may be admitted to NAVPERSCOM buildings at any time upon presentation of their official agency credentials:

- FBI
- Military Intelligence (Army)
- Naval Criminal Investigative Service
- Office of Special Investigation (Air Force)
- Secret Service (Treasury Department)
- Criminal Investigation Command (Army)
- Defense Investigative Service (DIS)
- Defense Protective Service (DPS)
- Defense Criminal Investigative Service
- Counterintelligence Credentials (USMC)
- U.S. Marshall's Service.

3. Access to NAVPERSCOM spaces controlled by electronic access control must be approved and granted by NAVPERSCOM (PERS-534).

1306. PROPERTY PASSES. NAVPERSCOM (PERS-533) issues property passes. No government property is to be removed from NAVPERSCOM without proper authorization from NAVPERSCOM (PERS-533). When government property is returned, NAVPERSCOM (PERS-533) must be notified. All government property carried by persons entering or leaving NAVPERSCOM buildings is subject to inspection by Naval Support Activity (NAVSUPPACT) Mid-South Security and NAVPERSCOM (PERS-534).

1307. LOSS OF PROPERTY, THEFTS, AND OTHER IRREGULARITIES

1. Loss or theft of Government or personal property or evidence of tampering with office doors, desks, etc., must be reported to NAVSUPPACT Mid-South Security and NAVPERSCOM (PERS-534).

2. Persons creating a public nuisance, suspicious persons, or other irregularities occurring within NAVPERSCOM spaces will be reported to NAVSUPPACT Mid-South Security and NAVPERSCOM (PERS-534) immediately.

1308. PHOTOGRAPHY AND AUDIO RECORDING EQUIPMENT/DEVICES

a. The use of any type of personal photography equipment, (i.e., instamatic camera, video tape recorder, digital/film camera, or a cell phone camera), is strictly prohibited in all BUPERS/NAVPERSCOM buildings and spaces without the approval of the NAVPERSCOM, Security Manager, (PERS-534). Supervisors may permit use of personal photography equipment on special infrequent occasions such as retirement and award ceremonies. If an individual has in their possession government issued photography equipment, this equipment is to be used only for official use only.

b. The use of any type of personal audio recording device, (i.e., tape recorder, cell phone recorder, iPod, eavesdropping ear amplifier (except for use by personnel who have a hearing impaired handicap), is strictly prohibited in all BUPERS/ NAVPERSCOM buildings and spaces without the approval of NAVPERSCOM (PERS-534). If an individual has in their possession government issued audio recording device, this device is to be used only for official use only.

c. When an individual plans to use government furnished photography equipment and/or audio recording device while attending a conference, meeting or other, the individual in charge of the session must be totally aware and grant their approval prior to the use of this equipment/device.

d. Cameras and audio recording devices no matter what type, model, or brand are a serious information security risk. All command personnel must understand the security risk when using this type of equipment/device in the government work place. Personnel found using this equipment/device without approved authorization will have the equipment/device confiscated and could possibly face disciplinary action.

APPENDIX A

ACRONYMS AND DESCRIPTIONS

ACRONYM	DESCRIPTION
ACNPC	Assistant Commander, Navy Personnel Command
AIS	Automated Information System
AOR	Area of Responsibility
ASF	Auxiliary Security Force
ASSIST	Automated Systems Security Incident Support Team
CAC	Common Access Card
CAF	Central Adjudication Facility
CCR	Contract Client Representative
CD-ROM	Compact Disk - Read Only Memory
CERTS	Computer Emergency Response Teams
CHNAVPERS	Chief of Naval Personnel
CI	Counterintelligence
CIRTS	Computer Incident Response Teams
CJCS	Chairman, Joint Chiefs of Staff
CMS	Communications Material System
CNA	Computer Network Attack
CND	Computer Network Defense
COMNAVPERSCOM	Commander, Navy Personnel Command
COMSEC	Communications Security
CS	Critical Sensitive
DEFCON	Defense Condition
DISA	Defense Information Systems Agency
DOD	Department of Defense
DON	Department of the Navy
DSS	Defense Security Service
EBACS	Electronic Badging Access Control System
EKMS	Electronic Key Management System
EMPRS	Electronic Military Personnel Record System
ERC	Emergency Response Cell
FBI	Federal Bureau of Investigations
FOUO	For Official Use Only
GAO	General Accounting Office
GMT	General Military Training
GTN	Global Transportation Network
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer

ACRONYM	DESCRIPTION
IAVA	Information Assurance Vulnerability Alert
IG	Inspector General
INFOCON	Information Operations Condition
INFOSEC	Information Systems Security
IO	Information Operations
IOC	Initial Operational Capability
IP	Internet Protocol
IRR	Inactive Ready Reserves
ISP	Information Security Program
I&W	Indications and Warning
JTF-CND	Joint Task Force - Computer Network Defense
LAA	Limited Access Authorization
LAN	Local Area Network
LEA	Law Enforcement Agency
LRA	Local Registration Authority
NAF	Nonappropriated Fund
NATO	North American Treaty Organization
NAVPERSCOM	Navy Personnel Command
NAVSUPPACT	Naval Support Activity
NAVCRIMINVSVC	Naval Criminal Investigative Service
NCS	Noncritical-Sensitive
NCTF-CND	Navy Computer Task Force - Computer Network Defense
NIPC	National Infrastructure Protection Center
NIPRNET	Non-Classified Internet Protocol Router Network
NISP	National Industrial Security Program
NMCI	Navy Marine Corps Internet
NPRST	Navy Personnel Research, Studies, and Technology
NSA	National Security Agency
NSI	National Security Information
NSM	Network Security Manager
OCA	Original Classification Authority
OJT	On-the-Job-Training
OPSEC	Operational Security
PKI	Public Key Infrastructure
POC	Point of Contact
PSI	Personnel Security Investigations
PSP	Personnel Security Program
SAP	Special Access Programs

ACRONYM	DESCRIPTION
SCMSRO	Staff Communications Security Material System Responsibility Officer
SA	Special Assistants
SCI	Sensitive Compartmented Information
SECDEF	Secretary of Defense
SIOP-ESI	Single Integrated Operation Plan - Extremely Sensitive Information
SIPRNET	Secret Internet Protocol Router Network
SORTS	Status of Resources and Training System
SS	Special Sensitive
SSA	Security Servicing Agreements
STE	Secure Telephone Equipment
STU-III	Secure Telephone Unit
TA	Trusted Agent
TEMPEST	Transient Electro-Magnetic Pulse Emanation Standard

APPENDIX B

FORMS AVAILABILITY

1. Following forms are used in conjunction with NAVPERSCOM ISP and are available at the below Web sites.

a. NAVPERS 5520/6 (Rev. 9-05), Request for Security Access is available at https://navalforms.daps.dla.mil/.

b. OPNAV 5216/10 (Rev. 6-78), Correspondence/Material Control Sheet, OPNAV 5510/413 (Rev. 1-94), Personnel Security Action Request, OPNAV 5511/10 (Rev. 12-89), Record of Receipt, OPNAV 5511/12 (Rev. 8-75), Classified Material Destruction Report, OPNAV 5511/13 (Rev. 1-76), Record of Disclosure, OPNAV 5511/14 (Rev. 9-05), Security Termination Statement, OPNAV 5511/27 (Rev. 11-92), Briefing/Rebriefing/Debriefing Certificate, OPNAV 5511/51 (5-80), Security Discrepancy Notice, and OPNAV 5521/27 (Rev. 9-92), Visit Request/Visitor Clearance Data are available at http://doni.daps.dla.mil/.

c. SF 700 (8-85), Security Container Information, SF 701 (8-85), Activity Security Checklist, SF 702 (8-85), Security Container Check Sheet, SF 703 (8-85), Top Secret Cover Sheet, SF 704 (8-85), Secret Cover Sheet, and SF 705 (8-85), Confidential Cover Sheet are available at http://www.dtic.mil/whs/directives/infomgt/forms/sfofforms.htm.

d. DD 372 (FEB 05), Request for Verification of Birth, is available at http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm.

e. FS-240, Report of Birth Abroad of a Citizen of the United States of America, FS-545, Certification of Birth, and DS-1350, Certification of Birth are available from State Department (Passport Office - Telephone Number (202) 647-0518).